patenttitoimisto/patent agency
KESPAT OY

Rekisteröidyt patenttiasiamiehet
Registered Patent Attorneys:
* Kimmo Helke
Anssi Kurkinen
Tuomo Kuivala

* Suomen Patenttiasiamies-yhdistys ry:n jäsen
Member of the Association of Finnish Patent Attorneys

European Patent Attorney
European Trademark Attorney
Yhteisömerkkiasiamies, OHIM

FICPI

By fax & mail to: +46 8 667 7288

PATENT- OCH REGISTRERINGSVERKET

Box 5055

S-10242 STOCKHOLM
SVERIGE

13 April 2004

VIITTEENNE
Your ref:

VIITTEEMME
Our ref: **PCT183 /470**

International Application No. PCT/FI2003/000282; Filing date: 14.4.2003 ;"System in a Digital Wireless Data Communication Network for Arranging End-to-end Encryption and Corresponding Terminal Equipment"; Priority: FI 20025018/23.4.2002; Applicant: Nokia Corporation et al

REPLY TO THE WRITTEN OPINION

Dear Sirs

Please find enclosed our reply to the Written Opinion on the above referenced application.

Yours faithfully

KESPAT OY

Tuomo Kuivala

ENC. Reply (comments 2 pages)

Postiosoite:
PL 601
40101 Jyväskylä
Käyntiosoite:
Vapaudenkatu 60

Address:
P.O.Box 601
FIN-40101 Jyväskylä
Finland

Puhelin/Telephone
+358 14 338 5500
Telefax: +358 14 338 5550
www.kespat.fi
mail@kespat.fi

Kaupparekisteri/
Trade reg.
339.648
Kotipaikka/
Registered in Jyväskylä

Int.appl. PCT/FI2003/000282; Nokia Corporation et al
Our ref: PCT183/470 TK

REPLY TO THE WRITTEN OPINION DATED 17-02-2004 – Rune Bengtsson / OGU

Document listed in Written Opinion:

D1: US 6151677 A

Applicant doesn't see any reasons to amend the original claims because the system according to the invention has to be considered as novel with an inventive step for arranging end-to-end (e2e) encryption in a digital wireless data communication network. Also, the terminal equipment according to claim 5 meets novelty with an inventive step. Additionally, there are no need to do any further descriptions relating to the claims; the invention has a clear difference to the document D1.

The Examiner states that document D1 presents a system of according to the invention in a digital wireless data communication network for arranging end-to-end encryption. Applicant respectfully traverses this opinion.

Document D1 presents a solution in which a security module has been arranged in connection with the terminal device as **statically**. The security module includes a processor devices in connection of which executed encryption program including encryption and decryption algorithms is also essentially static or at least in extremely inconveniently way updateable. This is due because the encryption program is a **hardware level program** i.e. firmware (column 3, lines 43 – 52). Additional to the static nature of the encryption algorithms refers also the reason that the encryption engine has been implemented in **hardware level being FPGA** (column 3, lines 56 – 57). Furthermore, to the static arrangement also refers the reason that the security module has been arranged to a single integration circuit (column 4, lines 65 – 67.

In D1 the security program (including encryption algorithms) has been presented to store in smartcard IC. From there the security program has been loaded to the FPGA when encryption has been wanted for execution. However, the smartcard IC has been integrated in this case statically to the security module on the device. This has been done especially due to the security reasons when interpreting the document as whole.

Applicant argues that a system according to the invention includes a novelty with an inventive step. In document D1 there is not at all hints to the **dynamic application environment that can be update from network** according to the invention. Any references for that in which encryption applications would be possible to download from the communication network or control there have not been presented in document D1. This is the main concept of the subject invention and this has been defined sufficient clearly in the claim 1.

The problem which has been solved in the subject invention is the one that manufacturers of the pieces of terminal equipment don't want be conscious at all about the encryption algorithms and methods used by the end users. In the way of document D1 this kind of problem can't be solve. In that the manufacturer of the terminal device must still deliver to the terminal device the security applications wanted by the client/end user. Due to the static nature

this have to deal out in the manufacturing phase of the terminal equipment. If these applications would leave out from the terminal device by the manufacturer, arranging of them as firmware implementation by the user would be considerably difficult or even impossible.

It must be notice that the question is totally different in the invention described in the subject application and document D1. In the D1 there are essentially static environment for which in the state-of-the-art –section of the subject application are also referred. In the subject invention question is to arrange the dynamic security application and its operating environment to the terminal device.

In the system according to the invention the end user can download to his terminal device the security application which one he just desires. To the terminal device has then been arranged sufficient services, interfaces and application environment for downloading of the security applications and for controlling of them. From the document D1 can't be found this kind of application environment in which the end user could "tailor" anything for him. Furthermore, there are no mention in the document D1 how the updating of the security application of the terminal device would be dealt out.

When comparing the subject invention and the solution described in document D1 our main conclusion is that security application implemented by firmware and executing that with the microprocessor is not same matter if the dynamic security application would download from the communication network for updating and executing that in Java virtual environment. By microprocessors have been executed security algorithms latest 20 years when in the embedded environment with Java machine not yet at all in this connection.

Several parties are attained advantages by the system and terminal equipment according to the invention. Firstly, for the terminal manufacturers, the system makes possible the ignorance of the security algorithms that have been wanted by the end user. Secondly, for the end user, system makes possible the freedom of choice to the algorithms wanted by him. Thanks to this a logistic advantage has been achieved, since batches of terminal equipment are not now tied to any particular security model.

The Examiner is also respectfully asked to take notice of the claims 2 and 3 in which have been defined that the terminal equipment is adapted to run applications according to the J2ME specification and configured in accordance with the MIDP specification. Also by these feature have been reached advantage, because these open for several parties possibility to implement security applications in the terminal equipment without any special hardware level knowledge or FPGA programming skills.

Also the claim 4 includes an inventive step with novelty because there are not any hints in document D1 to download applications in a self-organizing manner. This feature is also very useful because now there are no need for the user to manage terminal's security algorithms.

According to the above arguments a positive statement with regard to novelty and inventive step is requested.